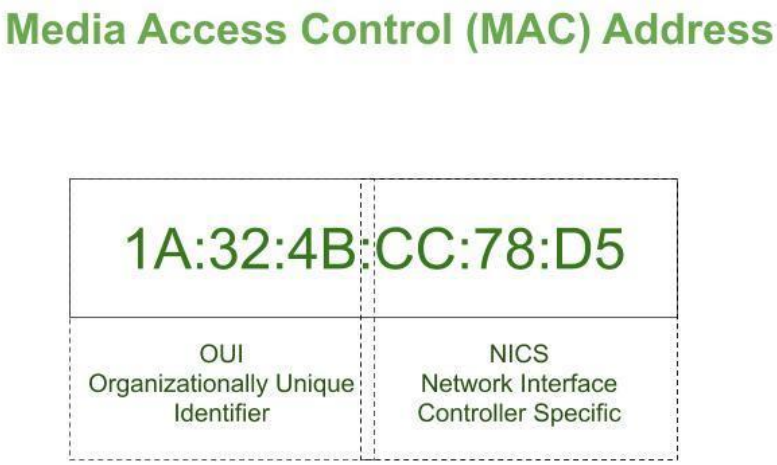
MAC stands for **Media Access Control.**

MAC address is defined as the **identification number for the hardware**. In general, the network interface cards (NIC) of each computer such as Wi-Fi Card, Bluetooth or Ethernet Card has unchangeable MAC address embedded by the vendor at the time of manufacturing. Dell, Nortel, Belkin, and Cisco are some of the well-known NIC manufacturers. One can change the given default address of the device by replacing the NIC cards.



Characteristics of MAC

- The MAC address that is considered to be the distinguishing number of the hardware is **globally unique.** This lets us identify each device within a connected network.
- The total length MAC address in **byte is 6 (or 48 bits)**. According to the IEEE 802 standards, this address is written in three commonly used formats:
    - Six two-digits hexadecimals separated by hyphens (-) like 45-67-89-AB-12-CD .
    - Six two-digits hexadecimals separated by colons (:) like 45:67:89:AB:DE:23 .
    - Three four-digits hexadecimals separated by dots (.) like ABCD.4567.1238 .
- The left 24 bits (3 bytes) of the address is termed as **Organizationally Unique Identifier (OUI) number.** This OUI number is assigned by **Internet Assigned**

Number Authority (IANA). This globally unique OUI number will always remain the same for NICs manufactured by the same company. The right 24 bits (3 bytes) of the address is termed as **Network Interface Controller Specific (NICS),** which is responsible for communication either by using cables or wirelessly over a computer network.

- Some devices that exist on this second layer are NIC cards, bridges and switches. This layer is also responsible for error free data transmission over the Physical layer under LAN transmissions. If we refer to our Open Systems Interconnection (OSI) network model, we will find that MAC addresses in the medium access control protocol sub-layer **uses data link layer**.

Advantages of MAC

- The devices that connect to the network have no **free attachment cost** associated with it.
- The router or switch has policy set on them. Either it has permitted equipment attached or non-permitted equipment attached irrespective of the person attaching it.
- The MAC addresses for all the devices on the same network subnet are different. Hence, **Diagnosing Network issues** relating to IP address, etc. are easy because of the usefulness of MAC Addresses.
- A network administrator feels **reliability** in identifying senders and receivers of data on the network with the help of MAC address. The only reason behind is that unlike dynamic IP addresses, the MAC addresses doesn't change from time to time.

Disadvantages of MAC

- Due to the reason that the first three bytes (OUI) for a MAC address reserved for the manufacturer, therefore it is limited for having only be **2^24 unique addresses** per OUI by the same manufacturer.
- We can say **spoofing is easy** for MAC address filtering. One can act in disguise and just listen to and from permitted MAC addresses because of the broadcast nature of ethernet.
- In most cases an **intruder can obtain access** to the network by constantly changing his MAC Address to a one that is permitted.

Multiple Access Protocols in Computer Network

The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-

- Data Link Control
- Multiple Access Control

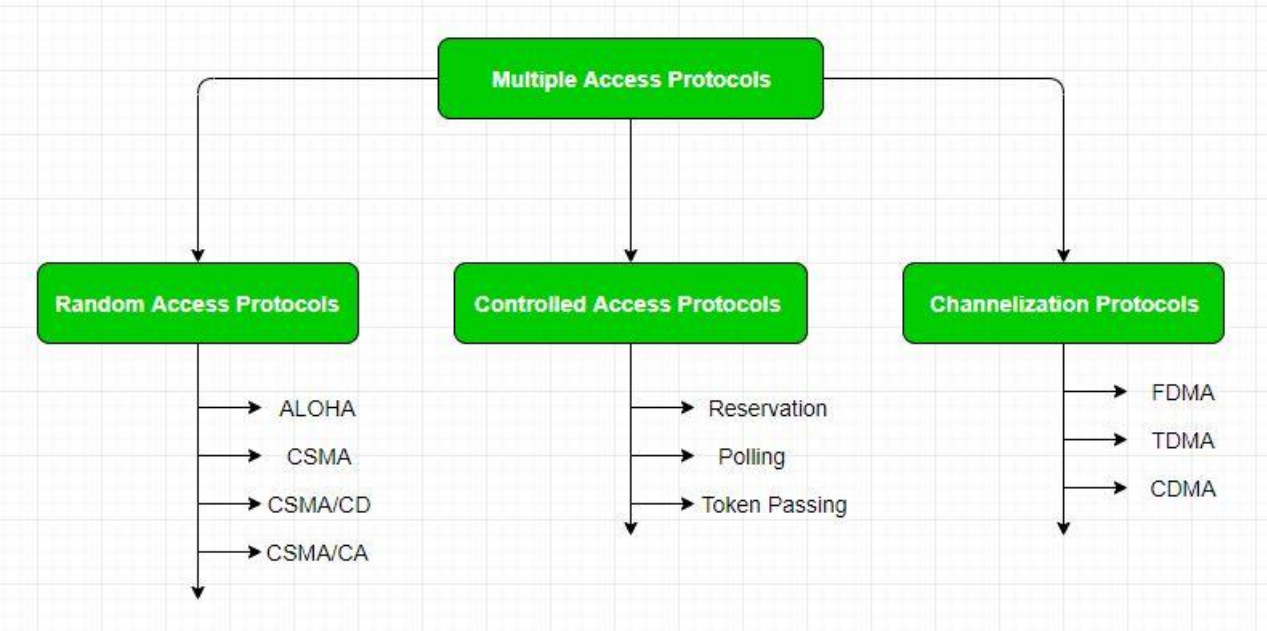
Data Link control –

The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control.

Multiple Access Control –

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there are no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created (data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.

Thus, protocols are required for sharing data on non-dedicated channels. Multiple access protocols can be subdivided further as –



Random Access Protocol

In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state (idle or busy). It has two features:

1. There is no fixed time for sending data
2. There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

(a) ALOHA –

It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

- **Pure Aloha:**

  When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time, then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.

Vulnerable Time = 2* Frame transmission time

Throughput = G exp{-2*G}

Maximum throughput = 0.184 for G=0.5

- **Slotted Aloha:**

  It is similar to pure aloha, except that we divide time into slots and sending of data

is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

Vulnerable Time = Frame transmission time

Throughput = G exp{-*G}

Maximum throughput = 0.368 for G=1

(b) CSMA – Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However, there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.
CSMA access modes-

- **1-persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally (with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

(c) CSMA/CD – Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected.
The CSMA method does not tell us what to do in case there is a collision. Carrier sense multiple access with collision detection (CSMA/CD) adds to the CSMA algorithm to deal with the collision. In CSMA/CD, the size of a frame must be large enough so that collision can be detected by the sender while sending the frame. So, the frame transmission delay must be at least *two times* the maximum propagation delay. Assume some station transmitted data packet and successfully get to the destination but it is just the *Best Case*, so we have to take the *Worst Case* scenario in which there will be contention slots. Contention slots are those slots that are not

able to transmit their journey due to the collision. Suppose station A transmitted data but collide and the worst-case time wasted is **2Tp** and then some station B found out a way to transmit the data so it took (As shown in Figure)

Tp (propagation delay) + Tt (transmission time)

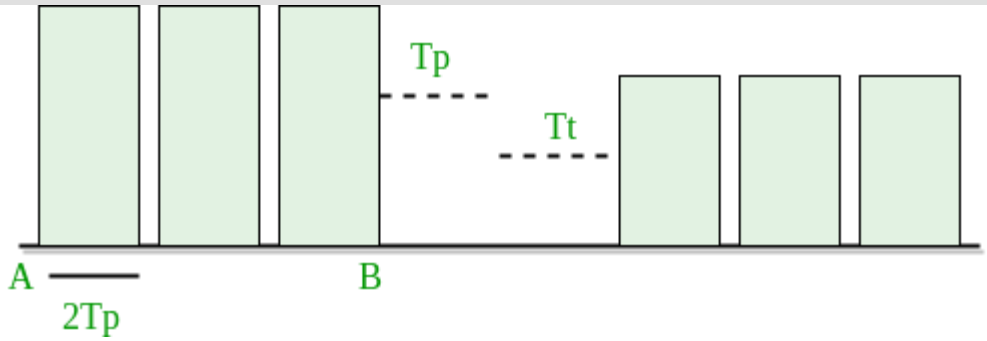
Now we don't know how many contention slots, so we consider the worst-case to be of **n** contention slots.

Efficiency = Tt / (C*2*Tp + Tt + Tp)

Tt - transmission time

Tp - propagation time

C - number of collision



In CSMA/CD, for success, only 1 station should transmit while others shouldn't. Let p be the probability to transmit data successfully.

P(success) = $nC1 * p * (1-p)^{n-1}$ (by using Binomial distribution)

For max P(success), differentiate with respect to p and equate to zero (to get maxima and minima).

We get P(max) = 1/e

Number of times we need to try before getting 1st success

1/P(MAX) = 1/(1/e) = e

Here number of times we need to try (C) = e. Put a = Tt/Tp and divide by T in Efficiency = Tt / (C* 2 * Tp + Tt + Tp) We get,

Efficiency = 1/(e*2a + 1 + a)

a = Tp/Tt

e = 2.72

Now

Efficiency = 1/(1 + 6.44a)

Further Analysis of Efficiency:

Efficiency = 1/ (1 + 6.44a)

= 1/ {1 + 6.44(Tp/Tt)}

= 1/ {1 + 6.44((distance/speed)/ (packet length/Bandwidth))}

= 1/ {1+ 6.44 ((distance * bandwidth)/ (speed*packet length))}

(d) CSMA/CA – Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal (its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However, it is not so in wired networks, so CSMA/CA is used in this case.
CSMA/CA avoids collision by:

1. **Interframe space –** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time, it again checks the medium for being idle. The IFS duration depends on the priority of station.
2. **Contention Window –** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
3. **Acknowledgement –** The sender re-transmits the data if acknowledgement is not received before time-out.

Controlled Access Protocols in Computer Network

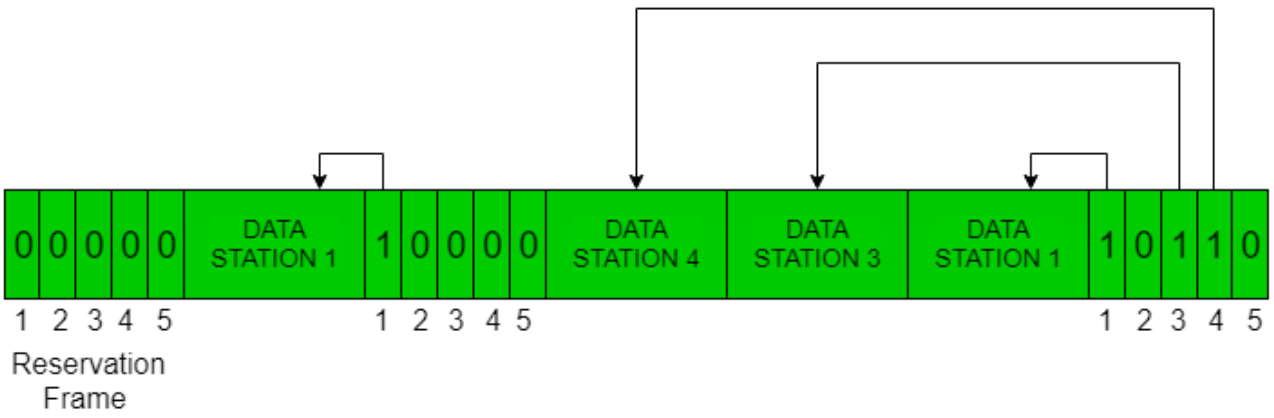
In controlled access, the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time, to avoid the collision of messages on a shared medium. The three controlled-access methods are:

1. Reservation
2. Polling
3. Token Passing

Reservation

- In the reservation method, a station needs to make a reservation before sending data.
- The timeline has two kinds of periods:
  1. Reservation interval of fixed time length
  2. Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
- In general, i th station may announce that it has a frame to send by inserting a 1 bit into i th slot. After all N slots have been checked, each station knows which stations wish to transmit.
- The stations which have reserved their slots transfer their frames in that order.
- After data transmission period, next reservation interval begins.
- Since everyone agrees on who goes next, there will never be any collisions.

The following figure shows a situation with five stations and a five-slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.



Advantages of Reservation:

- The main advantage of reservation is *high rates and low rates of data accessing* time of the respective channel can be predicated easily. Here time and rates are fixed.
- Priorities can be set to provide speedier access from secondary.
- Predictable network performance: Reservation-based access methods can provide predictable network performance, which is important in applications where latency and jitter must be minimized, such as in real-time video or audio streaming.
- **Reduced contention:** Reservation-based access methods can reduce contention for network resources, as access to the network is pre-allocated based on reservation requests. This can improve network efficiency and reduce packet loss.
- **Quality of Service (QoS) support**: Reservation-based access methods can support QoS requirements, by providing different reservation types for different types of traffic, such as voice, video, or data. This can ensure that high-priority traffic is given preferential treatment over lower-priority traffic.
- **Efficient use of bandwidth**: Reservation-based access methods can enable more efficient use of available bandwidth, as they allow for time and frequency multiplexing of different reservation requests on the same channel.
- **Support for multimedia applications:** Reservation-based access methods are well-suited to support multimedia applications that require guaranteed network resources, such as bandwidth and latency, to ensure high-quality performance.

Channelization

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA) –** The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA) –** In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However, there is an overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.

- **Code Division Multiple Access (CDMA) –** One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.

- **Orthogonal Frequency Division Multiple Access (OFDMA) –** In OFDMA the available bandwidth is divided into small subcarriers in order to increase the overall performance, Now the data is transmitted through these small subcarriers. it is widely used in the 5G technology.

Advantages:

- Increase in efficiency
- High data rates
- Good for multimedia traffic

Disadvantages:

- Complex to implement
- High peak to power ratio

- **Spatial Division Multiple Access (SDMA) –** SDMA uses multiple antennas at the transmitter and receiver to separate the signals of multiple users that are located in different spatial directions. This technique is commonly used in MIMO (Multiple-Input, Multiple-Output) wireless communication systems.

Advantages:

- Frequency band uses effectively
- The overall signal quality will be improved
- The overall data rate will be increased

Disadvantages:

- It is complex to implement
- It require the accurate information about the channel

Features of multiple access protocols:

Contention-based access: Multiple access protocols are typically contention-based, meaning that multiple devices compete for access to the communication channel. This can lead to collisions if two or more devices transmit at the same time, which can result in data loss and decreased network performance.

Carrier Sense Multiple Access (CSMA): CSMA is a widely used multiple access protocol in which devices listen for carrier signals on the communication channel before transmitting. If a carrier signal is detected, the device waits for a random amount of time before attempting to transmit to reduce the likelihood of collisions.

Collision Detection (CD): CD is a feature of some multiple access protocols that allows devices to detect when a collision has occurred and take appropriate action, such as backing off and retrying the transmission.

Collision Avoidance (CA): CA is a feature of some multiple access protocols that attempts to avoid collisions by assigning time slots to devices for transmission.

Token passing: Token passing is a multiple access protocol in which devices pass a special token between each other to gain access to the communication channel.

Devices can only transmit data when they hold the token, which ensures that only one device can transmit at a time.

Bandwidth utilization: Multiple access protocols can affect the overall bandwidth utilization of a network. For example, contention-based protocols may result in lower bandwidth utilization due to collisions, while token passing protocols may result in higher bandwidth utilization due to the controlled access to the communication channel.